IN THE CLAIMS:

Please amend the claims as follows:

1-29. (Canceled)

30. (Currently Amended) A method for monitoring user login activity for a server application, the method comprising:

(a) capturing communication data communicated in a network connecting a server application and a client without accessing or modifying the server application or the client and without affecting normal flow of network traffic;

(b) monitoring user login failures between the server application and the client during a predetermined time and based on the captured communication data; and

(c) detecting whether the number of user login failures exceeds a predetermined number.

31. (Original) The method of claim 30, wherein the communication data is communicated over a network selected from the group consisting of a global communication network, a wide area network, a local area network, and a wireless network.

32. (Previously Presented) The method of claim 30, wherein the communication data comprises an application protocol selected from the group consisting of hypertext transfer protocols, simple object access protocols, web distributed authoring and versioning protocols, wireless application protocols, file transfer protocols, Internet message access protocols, post office protocols, web services protocols, simple mail transfer protocols, structured hypertext transfer protocols, and web-mail protocols.

33. (Original) The method of claim 30, wherein the communication data can comprise HTTP requests from the client and HTTP responses from the server application.

34-36. (Canceled)

37. (Currently Amended) A system for monitoring user login activity for a server application, the method comprising:

(a) a network interface operable to capture communication data communicated in a network connecting a server application and a client, the network interface being separate from both the server application and the client;

(b) a detector operable to transparently monitor user login failures between the server application and the client during a predetermined time and based on the captured communicated data, and operable to detect when the number of user login failures exceeds a predetermined number.

38. (Original) The system of claim 37, wherein the communication data is communicated over a network selected from the group consisting of a global communication network, a wide area network, a local area network, and a wireless network.

39. (Previously Presented) The system of claim 37, wherein the communication data comprises an application protocol selected from the group consisting of hypertext transfer protocols, simple object access protocols, web distributed authoring and versioning protocols, wireless application protocols, file transfer protocols, Internet message access protocols, post office protocols, web services protocols, simple mail transfer protocols, structured hypertext transfer protocols, and web-mail protocols.

40. (Original) The system of claim 37, wherein the communication data can comprise HTTP requests from the client and HTTP responses from the server application.

41-43. (Canceled)

44. (Currently Amended) A computer program product comprising computer-executable instructions embodied in a computer-readable medium for performing steps comprising:

(a) capturing communication data communicated in a network connecting a server application and a client without accessing or modifying the server application or the client and without affecting normal flow of network traffic;

(b) monitoring user login failures between the server application and the client during a predetermined time and based on the captured communication data; and

(c) detecting when the number of user login failures exceeds a predetermined number.

45-71. (Canceled)

72. (Currently Amended) A method for monitoring user logoff activity for a server application, the method comprising:

(a) capturing communication data of a login session communicated in a network connecting a server application and a client without accessing or modifying the server application or the client and without affecting normal flow of network traffic;

(b) monitoring user logoff between the server application and the client based on the captured communication data;

(c) monitoring automatic session expiration between the server application and the client based on the captured communication data; and

(d) determining whether the client completes logoff before the session automatically expires.

73. (Original) The method of claim 72, wherein the communication data is communicated over a network selected from the group consisting of a global communication network, a wide area network, a local area network, and a wireless network.

74. (Previously Presented) The method of claim 72, wherein the communication data comprises an application protocol selected from the group consisting of hypertext transfer protocols, simple object access protocols, web distributed authoring and versioning protocols, wireless application protocols, file transfer protocols, Internet message access protocols, post office protocols, web services protocols, simple mail transfer protocols, structured hypertext transfer protocols, and web-mail protocols.

75. (Original) The method of claim 72, wherein the communication data can comprise HTTP requests from the client and HTTP responses from the server application.

76-78. (Canceled)

79. (Currently Amended) A system for monitoring user logoff activity for a server application, the method comprising:

(a) a network interface operable to capture communication data of a login session communicated in a network connecting a server application and a client, the network interface being separate from both the server application and the client;

(b) a detector operable to transparently monitor user logoff between the server application and the client based on the captured communication data, operable to monitor automatic session expiration between the server application and the client based on the captured communication data, and operable to determine whether the client completes logoff before the session automatically expires.

80. (Original) The system of claim 79, wherein the communication data is communicated over a network selected from the group consisting of a global communication network, a wide area network, a local area network, and a wireless network.

81. (Previously Presented) The system of claim 79, wherein the communication data comprises an application protocol selected from the group consisting of hypertext transfer protocols, simple object access protocols, web distributed authoring and versioning protocols, wireless application protocols, file transfer protocols, Internet message access protocols, post office protocols, web services protocols, simple mail transfer protocols, structured hypertext transfer protocols, and web-mail protocols.

82. (Original) The system of claim 79, wherein the communication data can comprise HTTP requests from the client and HTTP responses from the server application.

83-85. (Canceled)

86. (Currently Amended) A computer program product comprising computer-executable instructions embodied in a computer-readable medium for performing steps comprising:

(a) capturing communication data of a login session communicated in a network connecting a server application and a client without accessing or modifying the server application or the client and without affecting normal flow of network traffic;

(b) monitoring user logoff between the server application and the client based on the captured communication data;

(c) monitoring automatic session expiration between the server application and the client based on the captured communication data; and

(d) determining whether the client completes logoff before the session automatically expires.

87-92. (Canceled)

93. (Currently Amended) A method for monitoring simultaneous logins for a server application, the method comprising:

(a) capturing communication data communicated in a network connecting a server application and at least one client without accessing or modifying the server application or the client and without affecting normal flow of network traffic, wherein the captured communication data is associated with first and second user login sessions for first and second users, respectively, of the server application;

(b) monitoring the captured communication data associated with the first and second user login sessions; and

(c) determining whether the second user login session occurs during the first user login session when the user of the first and second login session are identical.

94. (Original) The method of claim 93, comprising selectively generating an alert based upon whether the second user login session occurs during the first user login session when the user of the first and second login session are identical.

95. (Original) The method of claim 93, wherein the first and second login sessions communicate over a network selected from the group consisting of a global communication network, a wide area network, a local area network, and a wireless network.

96. (Previously Presented) The method of claim 93, wherein the communication data comprises an application protocol selected from the group consisting of hypertext transfer protocols, simple object access protocols, web distributed authoring and versioning protocols, wireless application protocols, file transfer protocols, Internet message access protocols, post office protocols, web services protocols, simple mail transfer protocols, structured hypertext transfer protocols, and web-mail protocols.

97. (Canceled)

98. (Canceled)

99. (Currently Amended) A system for monitoring simultaneous logins for a server application, the method comprising:

(a) a network interface operable to capture communication data communicated in a network connecting a server application and at least one client, wherein the network interface is separate from both the server application and the client, and wherein the captured communication data is associated with first and second user login sessions for the first and second users, respectively, of the server application; and

(b) a detector operable to transparently monitor the captured communication data associated with the first and second user login sessions, and operable to determine whether the second user login session occurs during the first user login session when the user of the first and second login session are identical.

100. (Original) The system of claim 99, wherein the detector is operable to selectively generating an alert based upon whether the second user login session occurs during the first user login session when the user of the first and second login session are identical.

101. (Original) The system of claim 99, wherein the first and second login sessions communicate over a network selected from the group consisting of a global communication network, a wide area network, a local area network, and a wireless network.

102. (Previously Presented) The system of claim 99, wherein the communication data comprises an application protocol selected from the group consisting of hypertext transfer protocols, simple object access protocols, web distributed authoring and versioning protocols, wireless application protocols, file transfer protocols, Internet message access protocols, post office protocols, web services protocols, simple mail transfer protocols, structured hypertext transfer protocols, and web-mail protocols.

103. (Canceled)

104. (Canceled)

105. (Currently Amended) A computer program product comprising computer-executable instructions embodied in a computer-readable medium for performing steps comprising:

(a) capturing communication data communicated in a network connecting a server application and at least one client without accessing or modifying the server application or the client and without affecting normal flow of network traffic, wherein the captured communication data is associated with first and second user login sessions for first and second users, respectively, of the server application;

(b) monitoring the captured communication data associated with the first and second user login sessions; and

(c) determining whether the second user login session occurs during the first user login session when the user of the first and second login session are identical.

106-110. (Canceled)

111. (Currently Amended) A method of monitoring logins for a server application, the method comprising:

(a) designating a first login time for a client as a disallowed login time;

(b) determining a second login time for the client in communication data with a server application based on communication data captured from a network connecting the server application and the client without accessing or modifying the server application or the client and without affecting normal flow of network traffic;

(c) determining whether the second login time matches the first login time; and

(d) if the first and second login times match, indicating that the client in data communication with the server application is logging in at a disallowed login time.

112. (Original) The method of claim 111, if the login time for the client is disallowed, generating an alert.

113. (Original) The method of claim 111, wherein the server application communicates data over a network selected from the group consisting of a global communication network, a wide area network, a local area network, and a wireless network.

114. (Previously Presented) The method of claim 111, wherein the communication data comprises an application protocol selected from the group consisting of hypertext transfer protocols, simple object access protocols, web distributed authoring and versioning protocols, wireless application protocols, file transfer protocols, Internet message access protocols, post office protocols, web services protocols, simple mail transfer protocols, structured hypertext transfer protocols, and web-mail protocols.

115. (Original) The method of claim 111, wherein the data communicated with the server application can comprise HTTP requests from the client and HTTP responses from the server application.

116-118. (Canceled)

119. (Currently Amended) A system for monitoring logins for a server application, the method comprising:

(a) a network interface operable to monitor and capture communication data communicated between a server application and a client, the network interface being separate from both the server application and the client; and

(b) a detector operable to designate a first login time for a client as a disallowed login time, operable to determine a second login time for the client in communication data with a server application based on the communication data transparently captured from the network, operable to determine whether the second login time matches the first login time, and operable to indicating that the client in data communication with the server application is logging in at a disallowed login time, if the first and second login times match.

120. (Original) The system of claim 119, wherein the detector is operable to generate an alert if the login time for the client is disallowed.

121. (Original) The system of claim 119, wherein the server application communicates data over a network selected from the group consisting of a global communication network, a wide area network, a local area network, and a wireless network.

122. (Previously Presented) The system of claim 119, wherein the communication data comprises an application protocol selected from the group consisting of hypertext transfer protocols, simple object access protocols, web distributed authoring and versioning protocols, wireless application protocols, file transfer protocols, Internet message access protocols, post office protocols, web services protocols, simple mail transfer protocols, structured hypertext transfer protocols, and web-mail protocols.

123. (Original) The system of claim 119, wherein the data communicated with the server application can comprise HTTP requests from the client and HTTP responses from the server application.

124-126. (Canceled)

127. (Currently Amended) A computer program product comprising computer-executable instructions embodied in a computer-readable medium for performing steps comprising:

(a) designating a first login time for a client as a disallowed login time;

(b) determining a second login time for the client in data communication with a server application based on communication data captured from a network connecting the server application and the client without accessing or modifying the server application or the client and without affecting normal flow of network traffic;

(c) determining whether the second login time matches the first login time; and

(d) if the first and second login times match, indicating that the client in data communication with the server application is logging in at a disallowed login time.

128-134. (Canceled)

135. (Previously Presented) The method of claim 30 wherein capturing communication data includes copying the communication data communicated in the network connecting the server application and the client.

136. (Previously Presented) The method of claim 30 wherein the communication data contains a session identifier that identifies a session established between the server application and the client, and wherein monitoring user login failures includes identifying communication data containing the session identifier.

137. (Previously Presented) The system of claim 37 wherein the network interface is operable to copy the communication data being communicated in the network connecting the server application and the client.

138. (Previously Presented) The system of claim 37 wherein the communication data contains a session identifier that identifies a session established between the server application and the client, and wherein the detector is operable to identify communication data containing the session identifier.

139. (Previously Presented) The method of claim 72 wherein capturing communication data includes copying the communication data communicated in the network connecting the server application and the client.

140. (Previously Presented) The method of claim 72 wherein the communication data contains a session identifier that identifies a session established between the server application and the client, and wherein monitoring automatic session expiration includes identifying communication data containing the session identifier.

141. (Previously Presented) The system of claim 79 wherein the network interface is operable to copy the communication data being communicated in the network connecting the server application and the client.

142. (Previously Presented) The system of claim 79 wherein the communication data contains a session identifier that identifies a session established between the server application and the client, and wherein the detector is operable to identify communication data containing the session identifier.

143. (Previously Presented) The method of claim 93 wherein capturing communication data includes copying the communication data communicated in the network connecting the server application and the at least one client.

144. (Previously Presented) The method of claim 93 wherein the communication data contains two session identifiers that identify the two sessions established between the server application and one or two clients, and wherein monitoring the captured communication data includes identifying communication data containing the session identifiers.

145. (Previously Presented) The system of claim 99 wherein the network interface is operable to copy the communication data being communicated in the network connecting the server application and the at least client.

146. (Previously Presented) The system of claim 99 wherein the communication data contains two session identifiers that identify the two sessions established between the server application and one or two clients, and wherein monitoring the captured communication data includes identifying communication data containing the session identifiers.

147. (Previously Presented) The method of claim 111 wherein determining a second login time is based on communication data copied from the network connecting the server application and the client.

148. (Previously Presented) The method of claim 111 wherein the communication data contains a session identifier that identifies a session established between the server application and the client, and wherein determining a second login time includes identifying communication data containing the session identifier.

149. (Previously Presented) The system of claim 119 wherein the network interface is operable to copy the communication data being communicated in the network connecting the server application and the client.

150. (Previously Presented) The system of claim 119 wherein the communication data contains a session identifier that identifies a session established between the server application and the client, and wherein the detector is operable to identify communication data containing the session identifier.